Poznan University of Technology
Faculty of Computing and Telecommunications

michal.apolinarski[at]put.poznan.pl

Course: Application Security – laboratories

Lecturer: Michał Apolinarski, Ph.D.

Topic: Website Recon (OSINT Targeted on Web Applications)

Duration (on site): 180 min.

PREREQUISITES:

Knowledge of computer networks, operating systems and web apps.

GOALS:

- The aim of the class is to familiarize students with the OSINT (**O**pen **S**ource **Int**elligence) targeted on websites. In this lab, students will explore the fundamentals of website reconnaissance the first and crucial step in any security assessment. Without performing any attacks, participants will use publicly available tools and techniques to collect technical information about selected websites. Using passive and legal OSINT methods, students will examine domain structures, technology stacks, SSL configurations, exposed files, and more. This exercise is designed to sharpen analytical thinking and raise awareness of how much sensitive data can be unintentionally exposed online. It also demonstrates how much insight an attacker can gain without launching a single exploit and why minimizing metadata exposure is essential for security. Get ready to think like an attacker, without crossing the ethical line.
- Preparing a report of the performed tasks.

INSTRUCIONS (tasks for 1 person):

1. Remember that you should base on and use only public information accessible legally, Attention: You can't perform any type of active attacks, it's only a RECON. You may use for example:
    a. web browsers (*view source*, *devtools*, *inspectors*, *debuggers*, *add-ons*),
    b. operating systems network tools: *ping*, *tracert*, *Wireshark*, etc.
    c. on-line tools like: *dnschecker.org*, *who.is*, *Nslookup.io*, *dnsdumpster.com*, *mxtoolbox.com*, *subdomainfinder.c99.nl*, *wappalyzer.com*, *web-check.xyz*, *crt.sh*, *ssllabs.com*, *securityheaders.co*, *archive.org/web/* etc.
    d. search engines: *bing*, *google* (google dorks aka Google Hacking).
2. Choose your target, visit sites:
    a. https://www.put.poznan.pl/
    b. https://www.b-tu.de/
    c. https://web.unican.es/
    d. https://web.umons.ac.be/en/
    e. https://www.uphf.fr/
    f. https://www.uwasa.fi/fi
    g. ... (your idea, it can be any website☺)
3. For at least 2 of above sites try find as much as possible about technical issues (the more then better):
    a. website tech stack,
    b. IP addresses, DNS records, domain history / registrar, web server info (hosting provider), subdomains, geolocation,
    c. used CMS, dependencies and frameworks (additionally check for known vulnerabilities), information about developers,
    d. check web browser consol log (dev tools, network, storage), analyze requests, headers – look for any errors,
    e. check details about SSL (type, validation, CA, expire date), check if there is any unencrypted traffic,
    f. contents of /robots.txt file and sitemap.xml,
    g. check Google Dorks (indexed urls) like:
        i. publicly exposed documents[1],

[1] example: site:***domain*** ext:***doc*** | ext:***docx*** | ext:***odt*** | ext:***rtf*** | ext:***sxw*** | ext:***psw*** | ext:***ppt*** | ext:***pptx*** | ext:*pps* | ext:***csv***

ii. directory listing vulnerabilities[2],
iii. configuration / database / log files exposed,
iv. backup and old files,
v. login / signup pages,
vi. sql errors,
vii. php errors / warning,
viii. find subdomains / sub-subdomains,
ix. search in github / gitlab / wayback machine,

h. and so on…

4. Prepare and send to the lecturer a report of performed tasks (positive and false) with your results and analysis. Describe used tools and performed steps (add screenshots). Answer: what could be used for further attacks? Is the site vulnerable to OSINT? What should be improved?

REPORT:

- Should include a title page with full details of the student, course and exercise being reported.
- Should be carefully edited and provide evidence of the completion of all exercises confirmed by screenshots, answers and conclusions.
- Complete report should be send to the lecturer.

[2] example: site:***domain*** intitle:***index.of***